FLOURISH

FLOURISH is a multi-sector collaboration, helping to advance the successful implementation of Connected and Autonomous Vehicles (CAVs) in the UK, by developing services and capabilities that link user needs and system requirements.

The three year project, worth £5.5 million, seeks to develop products and services that maximise the benefits of CAVs for users and transport authorities. By adopting a user-centred approach, FLOURISH will achieve a better understanding of consumer demands and expectations, including the implications and challenges of an ageing society.

FLOURISH will address vulnerabilities in the technology powering CAVs, with a focus on the critical areas of cyber security and wireless communications. The project is trialled in the Bristol and South Gloucestershire region and is part funded from the Government’s £100 million Intelligent Mobility Fund, which is administered by the Centre for Connected and Autonomous Vehicles (CCAV) and delivered by the UK’s Innovation Agency, Innovate UK.

The FLOURISH consortium is made up of organisations from various sectors:

- ATKINS
- AIRBUS
- AEA
- UWE Bristol
- designability
- react ai
- TSS Transport Simulation Systems
- South Gloucestershire Council
- OPM
- age UK
- CATAPULT Transport Systems
- University of Bristol
- Bristol Robotics Laboratory
- Burges Salmon
Connected and Autonomous Vehicles are rapidly becoming a technological, social and economic reality. They will change the way we travel and the way we think about transport. Vehicles, roads, and the technology that connects them, will continue to become an integrated, communicative system rather than separate elements.

This throws up a whole host of challenges which go well beyond the design and manufacturing of the vehicles themselves. CAVs are, in essence, computers on wheels and, as such, they will generate vast quantities of data. This creates opportunities, but it also poses important questions about data security and the risk of cyber attacks, many of which we explore in this report.

It is critical that the legal and risk environment evolves to reflect these emerging challenges presented by the development of CAVs. Law and insurance must be an enabler of change, a force for good. They should unlock opportunities by balancing the collective good with individual requirements; providing clear accountabilities and risk allocation.

Cyber risk and data law are critical areas and are evolving as rapidly as the CAV technology itself. The UK Government has recognised this trend in recent years and has published three National Cyber Security Strategy papers in the past eight years and, most recently, a UK Digital Strategy.

This focus on cyber and data is welcome, particularly as the UK looks to become the world leader in driverless vehicle technology. If this ambition is to be realised, a secure cyber environment will be a prerequisite. In Chapter One we explore the question of why cyber security matters, before considering specifically the relationship between cyber security and CAV technology in Chapter Two.

The shape of regulation at international level is also rapidly developing. The European Union’s General Data Protection Regulation (GDPR) rules are due to take effect from May next year and these will have a significant bearing on the evolution of CAV technology. With the UK due to leave the EU less than a year later, questions arise as to the UK’s future relationship with the GDPR and that is an issue we explore in Chapter Three, in the context of the wider question of whether data is ‘the new fuel’.

This report identifies the shape of emerging issues and makes recommendations in Chapter Four pertaining to investment, data, consent and cyber security which we hope will contribute to the next stage of evolution of CAVs.

We are delighted to be involved with the FLOURISH project and look forward to publishing further reports that will drill down still further into these key issues.
Chapter One:
Why does Cyber Security matter

The issue of cyber security has become well established as a key pillar of Government security policy in recent times. The Government’s National Cyber Security Strategy 2016 – 2021 describes cyber security as “the protection of information systems (hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse”.1
Chapter One: Why does Cyber Security matter?

**UK Cyber Security Strategy**

The first UK Cyber Security Strategy was published by the then Labour Government in June 2009 and two further National Cyber Security Strategies have followed, in 2011 and 2016. In that first Cyber Security Strategy, the Government wrote that “[just] as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space.”

The theme of maintaining the UK’s competitive advantage has continued to be prevalent in the 2011 and 2016 Strategies, with Chancellor Philip Hammond writing in last year’s iteration that much of the UK’s prosperity “now depends on our ability to secure our technology, data and networks from the many threats we face” and that, while the threat of cyber security breaches will never be completely eliminated, we can “reduce the threat to a level that ensures we remain at the vanguard of the digital revolution.”

It is increasingly evident therefore that Government views the issue of cyber security not only as a security concern, but also as an economic imperative. This is reinforced by the inclusion of cyber security as one of the seven pillars of the Government’s UK Digital Strategy published in March 2017. The Digital Strategy commits the Government to “ensuring the UK is the best place to start and grow a digital business”.

With that goal in mind, Ministers will have been concerned by the findings of the Cyber Security Breaches Survey 2017, which found that almost half of all UK businesses suffered a cyber breach or attack in the past 12 months, rising to almost seven in ten amongst large businesses.

**Investment in cyber security**

Investment in cyber security is now a fact of life for most businesses. Two thirds of all UK firms have some level of cyber security spend. For micro/small firms, this averaged £2,600 over the past 12 months; for large businesses the average last year was £387,000. These are substantial costs to businesses and, viewed in this context, it is unsurprising that the Government is prepared to spend £1.9bn over the five year period from 2016 – 2021 to attempt to mitigate the cyber risks faced by businesses and ordinary citizens.

Given the cost to businesses of dealing with cyber attacks or breaches, the potential cost to Government of not investing in this area could potentially be significantly greater in terms of lost investment, jobs, productivity and tax receipts.

Connected and Autonomous Vehicles will incorporate a range of different technologies. These technologies will be required to integrate and interact with each other and, in an increasingly connected world, the external environment.

Alongside this, CAVs will generate enormous amounts of data with different and often multiple purposes. As CAVs evolve and become a reality on our roads, standards will need to be created which define the minimum security requirements embedded in the vehicle’s hardware, and what the boundaries are for software and connectivity.

The 2015 National Security Strategy (NSS) reaffirmed the cyber threat as a Tier One risk to UK interests. The level of threat is considered alongside Terrorism, War and Natural Disasters and whilst cyber security is not an issue that is in itself confined to CAVs, it is an issue which now pervades our daily lives.

Evidence received by the House of Lords Science and Technology Committee highlighted the extent to which CAVs will – and indeed already have – been subject to cyber security attacks.

The Committee recommended that the Centre for Connected and Autonomous Vehicles (CCAV) – with involvement from the National Cyber Security Centre – should play a coordinating role with regard to cyber security for CAVs, while the UK Government should also seek to facilitate coordinated international action to tackle the risks associated with cyber security.

In its recent report, FLOURISH partner Atkins stressed that "public acceptance of CAV technology and the safety and security of the vehicles rely on secure cyber systems.”

The security of the vehicles will, in part, be dependent on the protection of the data and information generated by CAVs. There will need to be a clear understanding as to where responsibility for security of information and systems sits in the supply chain.

The success of CAVs will also be dependent upon a consistent framework for cyber that is able to monitor and assess the effectiveness of security measures implemented. This will contribute to informing the position adopted by insurers and legislators in identifying the risks and the ways in which to mitigate them.

The FLOURISH project is addressing cyber security issues by design. For the successful adoption of CAVs it is crucial that the integrity of the information and communication systems is assured and validated.

**Automotive Cyber Security Standards**

Current progress is broadly as follows:

(a) EU: the EU Agency for Network and Information Security (an EU advisory body) has published a paper on good practices and recommendations;
(b) International; an SAE standard (J3061) and an ISO standard (ISO/IEC 21434) are in the process of being developed but have not yet been finalised; and
(c) USA: the National Highway Traffic Administration issued non-binding guidance in October 2016. A legislative bill relating to cyber security measures in cars was introduced in 2015 but its progress has since stalled.
Chapter Two: Cyber security and CAV technology

The advent of CAVs

The advent of CAVs has seen the potential for high-profile malicious cyber attacks on automotive systems. The wider adoption of CAVs is likely to see cyber criminals finding increasingly more innovative ways to attack and exploit the technology and the data. From hackers stealing vehicles remotely to stealing vast amounts of data and more sinister incidents of cyber attacks for other criminal activity, there are many risks that need to be considered.
The protection of CAVs from cyber attacks depends on the protection of a diverse range of systems and a large number of interfaces underlying the operation of CAVs, including cloud services, applications, car components, maintenance and diagnostic tools. This is key – in assessing the cyber risks posed by CAVs it is not sufficient to look at the CAV technology in isolation. Consideration must be given to the wider network - the infrastructure - in which CAVs operate.

Main cyber security threats to CAVs

- Loss of control over CAV assets or systems as the result of external cyber attack.
- Damage or loss of technology assets: loss of information in the cloud, loss of data, damage caused by a third party.
- Nefarious activity or abuse: denial of service attack, malicious code activity, manipulation of hardware and/or software, unauthorised access to systems.
- Unintentional damage: information leakage or sharing, using information from unreliable sources, inadequate design and planning or lack of adoption of standards.
- Network outage.
- Failures or malfunctions: failures or malfunctions of devices or systems, failures or disruptions to power supply, software bugs.
- Interception and hijackings: information interceptions, replay of messages, interfering radiations, session hijacking, network reconnaissance.

What standards exist today?

Cyber risks present challenges to the insurance and automotive industries. Insurers will need to consider new risks and offer appropriate policies. This will require insureds to meet prescribed standards of security to ensure policies are valid. Manufacturers will need to adapt to these standards and ensure appropriate testing (including penetration testing) and validation so that all components meet the standards before and after integration.

Cyber security standards within the automotive industry are generally in their early stages. While various industry and governmental bodies have recommended that such standards are developed at the earliest opportunity, there are very few national, regional or global standards currently in place. The first industry-led attempt to establish a framework of best practice in this space has been led by the Automotive Information Sharing and Analysis Center (Auto-ISAC) – a body established by the US-based Alliance of Automobile Manufacturers and the Association of Global Automakers in summer 2015.

The best practice guidelines set out by Auto-ISAC include seven core functions for cyber security in the automotive industry, including security by design, risk assessment and management, threat detection and protection, and collaboration and engagement with appropriate third parties.

Several initiatives have led to defining guidelines or rules to implement security in the automotive industry, however, none of them can be considered a standard yet, and the overall standards landscape has yet to achieve the level of completeness and consistency found in domains such as aircraft safety or smartcard security.

As is evident from the remarks of the UK Transport Minister, John Hayes MP, during the passage of the Vehicle Technology and Aviation Bill, discussions continue to take place at a high level on the development of these standards.

This is a core part of the FLOURISH project as the consortium looks to vulnerabilities in the technology powering CAVs, with a focus on the critical areas of cyber security and wireless communications.

Determining liability in the event of cyber attacks and responsibility for protecting against them will mean having a clear understanding of who or what was responsible in the supply chain, and if everyone involved was compliant with existing standards or frameworks.
Chapter Three: Data as the new fuel

“CAVs will be driven by data.”

In its Strategy on Cooperative Intelligent Transport Systems (C-ITS) the European Commission noted that data broadcast by C-ITS from vehicles “will, in principle, qualify as personal data as it will relate to an identified or identifiable natural person”. A 2016 report by McKinsey & Company highlighted that despite their privacy concerns, 71% of surveyed drivers willingly exchange their data for tangible benefits. This bodes well for the success of CAVs and the possibilities that they offer.

The flows of information can be broadly summarised as follows on the next page.
Chapter Three: Data as the new fuel

Central CAV system

Just like any modern vehicles, CAVs have in-built communication capabilities which are capable of recording and storing data. For example, their Electronic Control Units (ECUs) can record information about speed or journey distance. Many vehicles also contain Event Data Recorders (EDRs) which are capable of recording personal data (e.g. safety information such as the number of occupants in the vehicle if those individuals are identifiable).

The internal network systems of the vehicles, including Bluetooth and Wi-Fi connections, are also capable of storing the user’s personal data. This information will typically be stored in a central remote server.

A: User to the CAV and vice versa

CAV users will be required to input various personal information (such as name) and non-personal information (such as journey details). There may also be other ways for users of CAVs to input personal data or for CAVs to collect such data continuously without active user input; much of this could be sensitive personal data. For example, face recognition cameras, fingerprint recognition systems or the ability to record the user’s temperature in order to personalise the internal vehicle system.

The CAV system will in addition be constantly providing information to the user within the cab environment through increasingly sophisticated user displays. The cyber security design of this element of the human-machine interface is as important as the functionality and ergonomics.

B: Manufacturer to the CAV and vice versa

CAV manufacturers and technology providers will want to send any technological updates to the vehicles, some of which may be user-specific. Manufacturers will also be interested in obtaining certain vehicle information from the CAV such as road performance or fault and collision data in order to improve or update their technology.

C: One CAV to another and vice versa

One of the major benefits of CAVs is that they will help to reduce congestion and improve traffic flows. In order to do this, they will need to transmit traffic information, such as the location of road closures or accidents, to each other. They will therefore be able to disseminate traffic and geolocation data to other CAVs.

D: CAV to traffic authorities and vice versa

It is also important for CAVs to be able to store traffic information relating to congestion and road closures in order to facilitate the management of traffic. Traffic authorities will be interested in obtaining such information in order to monitor infrastructure conditions and to improve traffic flows.14

E: CAV to insurers or the police

It is highly likely that the police and insurance companies will be interested in obtaining data stored in the CAV’s ECUs and EDRs, particularly in the event of an accident. Such information will assist them in determining liability in the event of an accident; for example by disclosing the speed of the vehicle or analysing the vehicle’s sensor datasets at the time of the accident.

This information can also reveal user habits which will be useful to insurance companies.15

F: CAV to other stakeholders

It is likely that other stakeholders, such as researchers or Government bodies, including the Centre for Connected & Autonomous Vehicles and Innovate UK, will want to access the data stored and disseminated by CAVs for research and regulatory purposes. Such data might include anonymised personal data (i.e. data which would otherwise be classified as personal had it not been anonymised), vehicle information or traffic information.

Regulatory requirements underpinning a large-scale CAV operating environment are yet to be made clear but will need to be taken into account when designing cyber security structures. The regulatory position in connection with data sharing, encryption and access in the area of, for example, civil aviation (and related aspects of air traffic control and air accident investigation) gives some indication of the lines around which the regulatory position around CAVs could potentially develop.

At its simplest, the data involved in these data flows can be summarised into four types:

1. **Personal Data**
   - Any data which relate to a living individual who can be identified from those data or from those data and other information which is in possession (or likely to be) of the data controller.
   - Examples: Geolocation data, biometric identification data, collision data, user habits, safety data (such as the number of occupants in a vehicle if those individuals are identifiable).

2. **Special Category Data**
   - Any personal data which consist of information relating to racial or ethnic origin, political, religious or philosophical beliefs, trade union membership, physical or mental health/condition, genetic data, biometrics, sexual life/orientation or the commission (or alleged commission) of any offence or proceedings relating to such.
   - Examples: Collision information, biometric identification data, user habits (if, for example, this discloses the user’s health condition etc.).

3. **Commercially Sensitive Data**
   - Any data, that if disclosed, is likely to prejudice the commercial interests of any person.
   - Examples: Technological information (i.e. intellectual property information) stored in ECUs and EDRs.

4. **Non-sensitive Data**
   - Any data which falls outside the remit of commercially sensitive data, and which is not personal data or sensitive personal data.
   - Examples: Traffic information (i.e. congestion etc.), vehicle information (i.e. road performance, speed).

Figure 1: Data flows

Figure 2: Personal data

Figure 3: Non-personal data
Chapter Three: Data as the new fuel

Categorisation of data

The categorisation of this data is relevant because there are legislative frameworks which apply to protect data. As the regulatory approach to CAVs becomes clearer, it is possible that other categories of data could be designated for specified purposes (e.g. critical system/operational data captured and retained for the purposes of regulators).

The General Data Protection Regulation (GDPR)\textsuperscript{18} is due to come into effect on 25 May 2018 and represents a shift in the data protection landscape. It will replace the existing Data Protection Directive\textsuperscript{19} implemented into UK law by the Data Protection Act 1998.

The GDPR applies to the processing of personal data which can identify a living individual (i.e. data summarised in Figure 2). The GDPR places an emphasis on the customer’s interests and respect for an individual’s data. This has led to a tightening-up of a number of features of existing data protection legislation, extending its reach and increasing the fines for non-compliance.

Data collection is the cornerstone of the operation of CAVs and the importance of ensuring that this data can be used is clear. The data collected can be used to improve the safety and ability of CAVs, to improve traffic flow and to provide services back to users. However, the use of this data will inevitably raise the issue of data protection and protection of privacy. An appropriate balance between these sometimes competing considerations will need to be found so that the UK can appropriately exploit the potential opportunities in the use of this data and the CAV market.

In looking at how best to achieve this balance, one of the many questions that will need to be addressed is who the ‘data controller’ is in relation to the data collected, who else is entitled to access and use the data, and how that data may be shared between interested parties in the CAV ecosystem.

Under the current regime, the Data Protection Directive, any entity determining the purpose for and the manner in which personal data is collected or processed will be a ‘data controller’ and as such is subject to compliance with that legislation. Those processing personal data on behalf of a data controller are not caught by the Data Protection Directive and any obligations owed by data processors will be governed by the relevant contract. This changes under the GDPR and any entity processing personal data on behalf of data controllers will also have its own direct obligations under the GDPR.

Consequently, without further detailed consideration of the specific impact of the GDPR on the CAV ecosystem, it will therefore be key for stakeholders across the CAV chain to enter into carefully structured agreements identifying the distinct roles, responsibilities and accountabilities of each party. The nature of connected cars introduces the potential for multiple, joint and co-data controllers, as well as joint processors and sub-processors under the legislation.

There are clearly practical implications to the requirements under the GDPR which, understandably given the pace of change in this area, appears not to have been developed with the CAV ecosystem in mind. While CAV technology is still in the early stages of development, it may be necessary for the Government to legislate to ensure that the development of CAV technologies are appropriately supported and that any unequal balances of power do not result in unfair agreements limiting access to data or gridlock in reaching arrangements.

Data collection is the cornerstone of the operation of CAVs and the importance of ensuring that this data can be used is clear. The data collected can be used to improve the safety and ability of CAVs, to improve traffic flow and to provide services back to users.

Rail Cyber Security Standards

Cross-industry rail groups are actively working on cyber security. This includes the High Integrity Systems Group (HISG) hosted by RSSB (formerly the Rail Safety and Standards Board), and the Digital Railway Cyber Security Steering Group (DRCSSG) hosted by the Digital Railway programme at Network Rail. HISG is investigating what the cyber risks are and DRCSSG is looking into cyber security for future systems. RSSB also facilitates provision of cyber security guidance from the Department for Transport. To communicate with the industry, RSSB has formed the Cyber Security Advisory Group (CSAG) which published Network Rail’s Cyber Security Strategy in September 2013.

Standards currently utilised in the industry are generally not rail-specific:

(a) ISA/IEC 62443 (formerly ISA-99)
(b) BS EN 50126-1, BS EN 50126-2
(c) IEC 61508/ISO 27001

\textsuperscript{18} 19
Chapter Three:
Data as the new fuel

The incoming GDPR also raises a number of other considerations in terms of the practical arrangements and the interaction with the CAV ecosystem and CAV users.

Careful consideration will need to be given to the implications of:

- The requirement for the provision of privacy notices to users. Stakeholders will need to think about how these are best served to ensure the full understanding of the user, and thereby ensure full compliance with the GDPR.20
- User rights under the GDPR in relation to the right to be forgotten, the right to restriction of processing and the right to object to processing given the impact this could have on the operation of CAVs; the requirement for consent. This will need to include consideration of who needs to consent: whether this is the owner of the vehicle, the main user or additional passengers other than the main user, particularly further ahead in the future if fleets of autonomous vehicles become a reality. Consideration will also need to be given to whether grounds other than consent might be used to gather CAV data, for example, if a public good such as avoiding a collision can override privacy concerns of individuals.

For example, if a user opts out of sharing geolocation data, this will undermine certain safety features such as preventing speeding in speed limited areas, and will undermine traffic congestion information required to assist traffic management. In addition, data from event data records will become particularly important in the event of an accident or collision, and parties including manufacturers, insurers and law enforcement agencies may need access to this, in order to determine liability and continue to develop safety aspects of autonomous vehicles.

Whilst not addressing the CAV-ecosystem directly, there is flexibility within the GDPR which recognises that in certain circumstances, collection and processing activities are necessary notwithstanding the wishes of data subjects, for example in relation to specific use or the ‘right to be forgotten’. To provide the CAV supply-chain with certainty and to fully support the development of the technology, legislation to recognise the fundamental and strategic importance of personal data (for the purposes of, for example, public health, safety, national security) in the CAV ecosystem may well be necessary.

Why is this relevant for cyber security?

The GDPR requires data controllers and data processors to have in place ‘appropriate technical and organisational measures’ which “ensure appropriate security of personal data, including protection against unauthorised or harmful processing and against accidental loss, destruction or damage”.21 Any cyber attack on the systems controlling CAVs resulting in unauthorised access to or loss of personal data will necessarily raise the question as to whether such technical and organisational measures were in place. If such measures are found not to have been in place this will likely give rise to regulatory action by the data protection regulator, the Information Commissioner’s Office, claims from affected individuals and related claims from third parties (e.g. as between suppliers in the CAV supply chain).
Encryption

The GDPR provides specific suggestions for what kinds of security actions might be considered “appropriate to the risk”, including the pseudonymisation and encryption of personal data. In expressly stating these measures, the GDPR establishes encryption, among other measures, as a data protection standard that should be utilised. Additionally, while the GDPR goes on to state that if a breached organisation has “rendered data unintelligible” through protection measures such as encryption, then it can avoid the regulation’s breach notification requirement.

While encryption provides benefits in terms of cyber security – by preventing unauthorised bodies from being able to interpret the data - the focus on this in the GDPR provides a challenge for the development of CAVs. The nature of connected cars and the interdependency that is at the heart of their operation means that data needs to be passed on to a range of parties to ensure that the significant potential customer benefits are realised. However, encryption has the potential to provide a barrier to data sharing among every element in the connectivity chain.

The higher the level of encryption, the harder it is to provide data to third parties, either under GDPR or simply to make a CAV system workable. The challenge for those involved in the development of CAVs is to allow third party access to vehicle generated data in order to enhance the overall offering to consumers, but to do so in a way which is consistent with the principles of security, safety and privacy.

Additionally, encryption of data raises broader issues in relation to national security. Recent policy debate during the passage of the Investigatory Powers Bill in the UK Parliament included discussion on provisions on end-to-end encryption, with companies such as Apple voicing concern that provisions in the Bill could give the Government the power to demand Apple alters the way its messaging service works in order to allow security services to access messages. The final wording in the Act was amended as a result, to include provisions stipulating that companies must decrypt data where it is “practicable”.

On responding to the concerns of three parliamentary committees that considered the Bill, the Government made it clear that the amended Bill only requires Communications Services Providers to remove protection that they themselves have applied or that has been applied on their behalf. This means that the provisions rely on whether firms like Apple are deemed to apply end-to-end encryption to messages or if a user does it themselves, given that the software author does not have access to the key, rather only the users communicating. This ambiguity still requires further clarity, despite the passing of the Bill into law. While this Act relates to the powers available to the state to obtain communications data, similar disputes are not implausible in relation to CAVs: a car manufacturer could find themselves drawn into a scenario where law enforcement agencies demand access to a vehicle’s data to help them track a terrorist’s location, or demand that they override a vehicle that is being used by a terrorist as a weapon.

Following the terror attack on Westminster this year, Home Secretary Amber Rudd said that end-to-end encryption on messaging services such as WhatsApp and iMessage was “completely unacceptable” and that intelligence services must have “the ability to get into situations like encrypted WhatsApp”. While this debate is still ongoing, the potential legal need for CAV data to be decrypted by security services will need to be considered during the development of CAVs.

The CAV supply chain will also need to achieve a framework in which there is a high degree of confidence that all suppliers are GDPR compliant. Not only will this be necessary in the context of cyber security but more generally in the use of personal data provided to CAV manufacturers by users, generated by the CAVs or otherwise shared (to the extent permitted) between parties.

Data is a valuable commodity and recent high-profile cyber attacks have illustrated the ease with which cyber criminals have been able to access high volumes of personal data. CAVs have already been the subject of several high profile attacks and it is likely that the prevalence of attacks will increase. Being ready to address this issue through legislation and appropriate insurance is key to the successful adoption of CAVs. The Network and Information Systems (NIS) Directive, which aims to improve national cyber security capabilities, entered into force in August 2016.

The UK (along with other European Union Member States) will be required within 21 months to adopt a national network and information security strategy and establish a network and information security authority which can prevent, handle and respond to cyber threats and incidents.

As part of implementation, the UK will need, within a further six months (and subject to Brexit), to identify “operators of essential services” (which will be in critical sectors such as energy, transport, banking and health) which will be required to adopt risk management practices and place a further breach obligation on organisations which will have to report major cyber incidents to the national NIS authority.

It is likely that legislators will pay particular attention to CAV technologies, looking at the practical steps for security and ensuring compliance with the GDPR. Consequently, it is likely that CAV operators will be designated as “operators of essential services” within the UK and required to comply with the NIS Directive.
Chapter Three:  
Data as the new fuel

Changing landscape

The legislation in this area will of course be subject to change over time. We are likely to see developments in respect of:

- Brexit: as a result of the UK’s decision to leave the European Union and the ability for the UK to make changes to Regulations and legislation enacted to implement Directives from the European Union;
- Declaration of Amsterdam: under this agreement, the Netherlands, the European Commission, EU member states and the transport industry pledged to create a single set of rules and regulations to allow CAVs to be used on the roads;27
- The market: to respond to calls for legislation to address particular issues such as data sharing and cyber security;
- Technological change.

Implications of Brexit

It is worth considering in more detail the implications of Brexit for the GDPR, and what this might mean for future rules and regulations to allow CAVs to be used on the roads.

The GDPR was agreed by the European Parliament in April 2016 and will apply across the European Union (including the UK as a current member) from May 2018 without the need for any changes in UK domestic legislation. However, as a consequence of the EU Referendum there is a question mark over how long this legislation will remain in place when the UK Leaves the EU. The Government gave notice of its intention to leave the EU through triggering Article 50 in March 2017, putting the UK on track to exit by the end of March 2019 (or before, if no withdrawal agreement can be negotiated). If no action is taken, at this point GDPR would no longer be applicable in the UK.

However in reality, this situation is unlikely. The Government has committed through its white paper, ‘Legislating for the United Kingdom’s withdrawal from the European Union’ to transpose all existing EU legislation onto the UK statute book through the Great Repeal Bill. As stated by the Prime Minister, The Rt Hon Theresa May MP, in the foreword of this policy paper, “Our decision to convert the ‘acquis’ – the body of European legislation – into UK law at the moment we repeal the European Communities Act is an essential part of this plan.

This approach will provide maximum certainty as we leave the EU. The same rules and laws will apply on the day after exit as on the day before. It will then be for democratically elected representatives in the UK to decide on any changes to that law, after full scrutiny and proper debate.”28

In addition, during a House of Lords EU Home Affairs Sub-Committee evidence session, the Minister of State for Digital and Culture, The Rt Hon Matt Hancock MP said that the only way to ensure the UK can negotiate an uninterrupted and unhindered flow of data with the EU is to put GDPR into UK law, commenting that the UK is “matching them rather than asking them to match anything new from the UK”.

However, Hancock also said that there is the “potential to make the GDPR easier to comply with or more flexible, but we would want to do that only consistent with maintaining unhindered data flows within the data protection regime”. This leaves a series of questions for UK based organisations looking at CAV technologies, which it is hoped will be answered over the coming months as the Government begins to negotiate the UK’s exit from the EU:

- How will the new regulatory landscape develop after the UK leaves the EU and will it diverge from GDPR (including any subsequent development of GDPR through the case law of the European Court of Justice)?
- How will the UK view its future position regarding data exchanges with other jurisdictions that have data protection regimes such as the US, and will this impact on any divergence from the GDPR?
- What arrangements will exist for continuation (or not) in the longer term of the new obligations in the NIS Directive.

Given that GDPR applies to organisations that hold or use personal data of EU citizens, even if they are based outside of the EU, post-Brexit the majority of UK based organisations will still need to comply with the regulations whether or not the UK legislature subsequently amends or repeals the GDPR from UK legislation.

Once the UK has left the EU, decisions on future data regulation, including any changes to the GDPR, will be made without the UK. However, these decisions will still affect the UK and CAV operators who deal with personal data of EU citizens. How will the UK seek to influence this process? What does Brexit mean for the UK’s involvement in the Amsterdam Agreement and the creation of a single set of rules and regulations to allow CAVs to be used on the roads?

Once the UK has left the EU

We are likely to see developments in respect of:

- Brexit: as a result of the UK’s decision to leave the European Union and the ability for the UK to make changes to Regulations and legislation enacted to implement Directives from the European Union;
- Declaration of Amsterdam: under this agreement, the Netherlands, the European Commission, EU member states and the transport industry pledged to create a single set of rules and regulations to allow CAVs to be used on the roads;27
- The market: to respond to calls for legislation to address particular issues such as data sharing and cyber security;
- Technological change.

Cyber security standards within the aviation industry are more ‘mature’. The ‘gold-standard’ cyber security specifications in the aviation industry are the RTCA DO-326(A), DO-355 and DO-356 standards.
The pace of technological change and innovation in the CAV ecosystem is rapid. The potential benefits of CAVs will, in many cases, be life-changing and it is a focus of the FLOURISH project to explore the acceptance of CAVs by adopting a user-centred approach.

This report focuses on the practicalities of cyber security and data sharing; this is, as we have discussed, critical to the success of CAVs.

Clarity on the sharing of data and the development of cyber security standards will be fundamental to support the development and exploitation of the technology. However, it will also be key to exploring user-acceptance; providing clarity to users on how CAVs (and the CAV ecosystem) use their data and how they are protected from cyber attacks is likely to play an important role in ensuring the success of CAVs.
Recommendations

Data

- The Government should consult on the implications of the General Data Protection Regulation for connected and autonomous vehicles and access to data for third parties, as this will play a crucial role in the development of the technology. In particular, the Government should look at how the system of data controllers and processors will work in the context of autonomous vehicles; whether the standards of consent are appropriate in this context; and what role encryption can and should play in relation to CAV data.

- The ICO should produce further guidance on whether CAV data falls into either data processes for public health purposes in the public interest or for archiving purposes in scientific research, in order to clarify the extent of the “right to be forgotten” in this area.

- The Government should clarify its position on security services or other regulatory access to encrypted data, in order to allow for any need for security services or regulators to access CAV data to be taken into account during the development of the technology.

Consent

- The ICO should clarify what form of consent is required for use of ‘Special Categories’ under the GDPR, including whether or not an individual can provide consent on behalf of another individual.

- DCMS should work with stakeholders to establish necessary alternative legal bases to consent or permitted use for the processing of CAV data, for example where data is required to ensure the safety of CAVs.

Cyber Security

- The Government should also consult on cyber security issues raised by a connected transport ecosystem, to ensure that the unique risks are understood and the appropriate safeguards put in place when the technology is rolled out.

- The Government should clarify whether CAV operators will be designated as “operators of essential services” within the UK and therefore whether they are required to comply with the NIS Directive, including in the light of the Brexit negotiation outcome.

- The Government should clarify in other respects how it would intend to regulate the standards and operation of CAVs and CAV systems as they relate to data and data security so that they can be incorporated by design.

- Government and Industry should consider potential approaches to approvals and regulation of the supply chain including parts and maintenance organisations. This should draw on experience in equivalent industries and transport modes such as Rail (for example the approval of Entities in Charge of Maintenance) and Aviation (Maintenance Organisation Approvals and Production Organisation Approvals).

Investment

- The Government should continue to invest in the development of CAV technology, including through funding for creation of test facilities, and industry-led research and development projects.
References

6. Ibid
9. Atkins, Connected & Autonomous Vehicles: Introducing the Future of Mobility
10. Ibid
19. Directive 95/46/EC
20. Under the GDPR, consent must be freely given, specific, informed and an unambiguous indication of the individual’s wishes.
21. Under the GDPR, consent must be freely given, specific, informed and an unambiguous indication of the individual’s wishes.
22. Article 5, General Data Protection Regulation. Under the Data Protection Directive 95/46/EC this legal obligation applied only to data controllers. Under the GDPR it applies independently to both data controllers and data processors.
30. 64. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
31. Directive 95/46/EC